PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-191761
(43)Date of publication of application : 13.07.1999

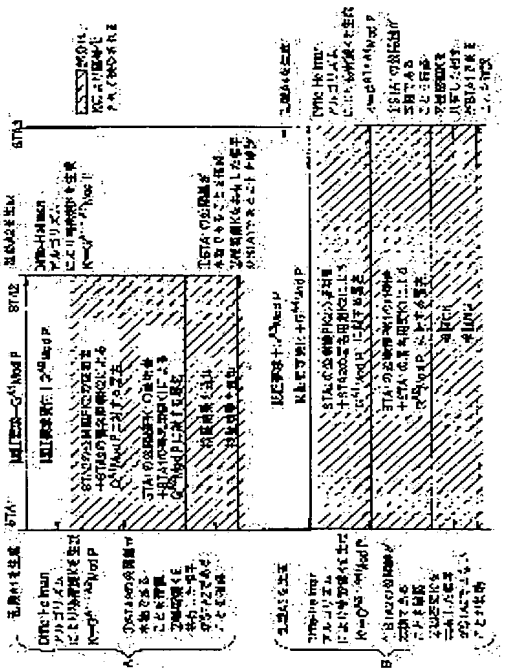
(51)Int.Cl. H04L 9/32
G09C 1/00

(21)Application number : 09-357158
(22)Date of filing : 25.12.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KUNO YUTAKA
KOBAYASHI TETSUTARO
MORITA HIKARI

(54) MUTUAL AUTHENTICATION METHOD AND DEVICE THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a mutual authentication method that keeps security against attacks and executes efficient authentication.
SOLUTION: A random number A1 is generated in a STAB, a GA1Mod P is sent to a SAT 2 by the Diffie-Hellman key delivery algorithm. The STA2 generates a random number A2 and sends GA2Mod P to the STA1. The STA1, STA2 obtain a shared key GA1.A2Mod P. The STA2 sends a certificate of a public key PK2 of the STA2 by an authentication station and a signature C2 of the GA1Mod P by a private key K2 to the STA1. The STA1 sends a certificate of a public key PK1 of the STA1 by an authentication station and a signature C1 of the GA2Mod P by a private key K1 to the STA2. The STA1, STA2 confirm the legitimacy of the public key based on the received information and authenticates the signatures with each other by using the respective public keys.



LEGAL STATUS

[Date of request for examination]	14.12.2000
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3253060
[Date of registration]	22.11.2001
[Number of appeal against examiner's decision of rejection]	

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－191761

(43)公開日　平成11年(1999)７月13日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｃ０９Ｃ	1/00	６４０Ｅ
					６４０Ｂ
			Ｈ０４Ｌ	9/00	６７５Ｄ

審査請求　未請求　請求項の数７　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－357158

(22)出願日　平成９年(1997)12月25日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　久埜　豊
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　小林　鉄太郎
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　森田　光
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】　相互認証方法及びその装置

(57)【要約】

【課題】　攻撃に対して安全であり、かつ効率的に行うことができる。

【解決手段】　ＳＴＡ１で乱数Ａ１を生成し、Diffie-Hellman鍵配送アルゴリズムによりG^A1 Mod PをＳＴＡ２へ送り、ＳＴＡ２ではＡ２を生成し、G^A2 Mod PをＳＴＡ１へ送り、ＳＴＡ１，ＳＴＡ２で共有鍵G^A1・A2 Mod Pを得る。ＳＴＡ２はＳＴＡ２の公開鍵ＰＫ２の認証局による証明書とその秘密鍵Ｋ２によるG^A1 Mod Pに対する署名Ｃ２をＳＴＡ１へ送り、ＳＴＡ１はその公開鍵ＰＫ１の証明書とその署名用鍵Ｋ１によるG^A2 Mod Pに対する署名Ｃ１をＳＴＡ２へ送る。各ＳＴＡ１，ＳＴＡ２では受信情報から、その公開鍵の正当性を確認し、かつその公開鍵で署名を検証する。

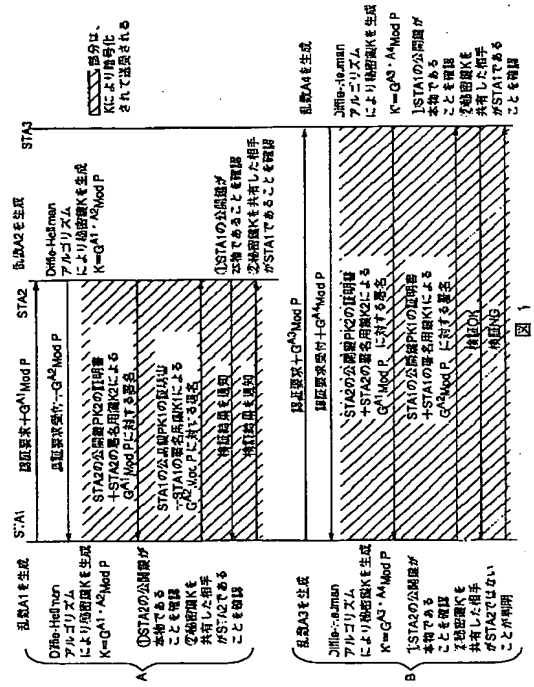


図１

【特許請求の範囲】
【請求項１】　２台の通信装置ＳＴＡ１、ＳＴＡ２の一方の通信装置ＳＴＡ１が乱数Ａ１を発生し、関数Ｆによって、Ｆ（Ａ１）を算出してＦ（Ａ１）を他方の通信装置ＳＴＡ２に送信し、
通信装置ＳＴＡ２が乱数Ａ２を発生し、関数Ｇによって、Ｇ（Ａ２）を算出してＧ（Ａ２）を通信装置ＳＴＡ１に送信し、
通信装置ＳＴＡ１は乱数Ａ１と、受信したＧ（Ａ２）から秘密鍵ＳＫを生成し、
通信装置ＳＴＡ２は乱数Ａ２と、受信したＦ（Ａ１）から秘密鍵ＳＫを生成し、
共有した秘密鍵ＳＫを用いた暗号通信を行う通信システムにおける相互認証方法において、
通信装置ＳＴＡ１は、
① 通信装置ＳＴＡ１のデジタル署名用鍵Ｋ１に対応する公開鍵ＰＫ１
② 認証局によるＰＫ１へのデジタル署名Ｂ１（以下、公開情報ＰＩと、認証局によるＰＩに対するデジタル署名の組のことを、ＰＩの証明書と呼ぶ。① と② はＳＴＡ１の公開鍵ＰＫ１の証明書Ｓ１である。）
③ Ｇ（Ａ２）の通信装置ＳＴＡ１の署名用鍵Ｋ１によるデジタル署名Ｃ１
を通信装置ＳＴＡ２に送信し、
通信装置ＳＴＡ２は
① 通信装置ＳＴＡ２のデジタル署名用鍵Ｋ２に対応する公開鍵ＰＫ２の証明書Ｓ２
② Ｆ（Ａ１）の通信装置ＳＴＡ２の署名用鍵Ｋ２によるデジタル署名Ｃ２
を通信装置ＳＴＡ１に送信し、通信装置ＳＴＡ１、ＳＴＡ２でそれぞれ受信した証明書とデジタル署名の検証を行うことを特徴とする相互認証方法。
【請求項２】　上記Ｇ（Ａ２）の署名用鍵Ｋ１によるデジタル署名Ｃ１は、Ｇ（Ａ２）を変数とする関数Ｈ（ＧＡ２）に対するＫ１によるデジタル署名であり、
上記Ｆ（Ａ１）の署名用鍵Ｋ２によるデジタル署名Ｃ２は、Ｆ（Ａ１）を変数とする関数Ｉ（Ｆ（Ａ１））に対するＫ２によるデジタル署名であることを特徴とする請求項１記載の相互認証方法。
【請求項３】　上記関数Ｈの変数として、上記乱数Ａ１を含み、上記関数Ｉの変数として上記乱数Ａ２を含むことを特徴とする請求項２記載の相互認証方法。
【請求項４】　２台の通信装置ＳＴＡ１、ＳＴＡ２の一方の通信装置ＳＴＡ１が公開鍵αを他方の通信装置ＳＴＡ２に送信し、
通信装置ＳＴＡ２が乱数Ａ２を発生し、関数Ｇによって、Ｇ（α、Ａ２）を算出してＧ（α、Ａ２）を通信装置ＳＴＡ１に送信し、
通信装置ＳＴＡ１は、Ｇ（α、Ａ２）から秘密鍵ＳＫを生成し、通信装置ＳＴＡ２はＡ２から秘密鍵ＳＫを生成し、
共有した秘密鍵ＳＫを用いた暗号通信を行う通信システムにおける相互認証方法において、
通信装置ＳＴＡ１は乱数Ａ１を発生し、
① 通信装置ＳＴＡ１のデジタル署名用鍵Ｋ１に対応する公開鍵ＰＫ１の証明書Ｓ１
② （Ａ１，Ｇ（α、Ａ２））の通信装置ＳＴＡ１の署名用鍵Ｋ１によるデジタル署名Ｃ１
③ 乱数Ａ１
を通信装置ＳＴＡ２に送信し、
通信装置ＳＴＡ２は
① 通信装置ＳＴＡ２のデジタル署名用鍵Ｋ２に対応する公開鍵ＰＫ２の証明書Ｓ２
② 関数Ｉを用いて算出される（Ａ１，Ｇ（α、Ａ２））の通信装置ＳＴＡ２の署名用鍵Ｋ２によるデジタル署名Ｃ２
を通信装置ＳＴＡ１に送信し、通信装置ＳＴＡ１、ＳＴＡ２でそれぞれ受信した証明書とデジタル署名の検証を行うことを特徴とする相互認証方法。
【請求項５】　上記（Ａ１，Ｇ（α、Ａ２））に対する署名用鍵Ｋ１によるデジタル署名Ｃ１は、（Ａ１，Ｇ（α、Ａ２））を変数とする関数Ｈ（Ａ１，Ｇ（α、Ａ２））に対するＫ１による署名であり、
上記（Ａ１，Ｇ（α、Ａ２））に対する署名用鍵Ｋ２によるデジタル署名Ｃ２は、（Ａ１，Ｇ（α、Ａ２））を変数とする関数Ｉ（Ａ１，Ｇ（α、Ａ２））に対するＫ２による署名であることを特徴とする請求項４記載の相互認証方法。
【請求項６】　乱数Ａｎ、共有秘密鍵ＳＫ、認証用公開鍵ＰＫｎの認証局の証明書、公開鍵ＰＫｎと対応する署名用秘密鍵Ｋｎ、相手通信装置から共有鍵配送時に受信した鍵配送用関数値Ｇ（Ａｉ）を記憶する記憶手段と、
上記乱数Ａｎを生成する乱数生成手段と、
上記乱数Ａｎを変数とする関数演算を行う鍵配送用演算手段と、
相手通信装置からの鍵配送用関数値Ｇ（Ａｉ）と乱数Ａｎとを用いて上記共有の秘密鍵ＳＫを生成する共有鍵生成手段と、
上記鍵配送用関数値Ｇ（Ａｉ）に対し上記署名用秘密鍵Ｋｎによるデジタル署名Ｃｎを生成する署名手段と、
相手通信装置からの公開鍵ＰＫｉに対する証明書からその公開鍵ＰＫｉの正当性を確認する公開鍵確認手段と、
上記相手通信装置からの鍵配送用関数値Ｇ（Ａｎ）に対する署名Ｃｉを上記公開鍵ＰＫｉで検証する署名検証手段と、
上記公開鍵確認手段の確認結果と、上記署名検証手段の検証結果とから相互認証に対する検証結果を生成する手段と、
上記鍵配送用演算手段の演算結果Ｆ（Ａｎ）、上記署名Ｃｎおよび上記公開鍵ＰＫｎの証明書、上記認証結果を

上記相手通信装置へ送信する送信手段と、
外部からの情報を受信する受信手段と、
上記各手段を制御し、順次処理を実行させる制御手段とを具備する相互認証用通信装置。
【請求項７】　鍵配送用公開鍵及び秘密鍵、相手通信装置からの暗号関数値Ｇ（α、Ａｉ）と乱数Ａｎ、共有秘密鍵ＳＫ、認証用公開鍵ＰＫｎの証明書Ｓｎ、そのＰＫｎと対応する署名用秘密鍵Ｋｎを記憶する記憶手段と、
鍵配送用乱数Ａｎを生成する乱数生成手段と、
相手通信装置からの公開鍵βにより上記乱数Ａｎを暗号化して暗号関数値Ｇ（β、Ａｎ）を得る暗号手段と、
相手通信装置からの暗号関数値Ｓｉ＝Ｇ（α、Ａｉ）と上記鍵配送用公開鍵αとを入力して、上記共有鍵ＳＫを生成する共有鍵生成手段と、
認証用乱数Ａｎ´を生成する乱数生成手段と、
上記認証用乱数Ａｎ´と、上記相手通信装置からの暗号関数値Ｓｉに対する上記署名用秘密鍵Ｋｎによりデジタル署名Ｃｎを生成する署名手段と、
相手通信装置からの公開鍵ＰＫｉに対する証明書からその公開鍵ＰＫｉの正当性を確認する公開鍵確認手段と、
上記相手通信装置からの暗号関数値Ｇ（α、Ａｉ）と乱数Ａｎ´に対する署名Ｃｉを上記公開鍵ＰＫｉで検証する署名検証手段と、
上記公開鍵確認手段の確認結果と、上記署名検証手段の検証結果とから相互認証に対する検証結果を生成する手段と、
上記鍵配送用公開鍵α、上記暗号関数値Ｇ（β、Ａｎ）、上記証明書Ｓｎ及び署名Ｃｎ、上記相互認証検証結果を相手通信装置に送信する送信手段と、
外部からの情報を受信する受信手段と、
上記各手段を制御し、順次処理を実行させる制御手段とを具備する相互認証用通信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、交信により共通の秘密鍵を生成し、その秘密鍵により暗号通信を行う通信システムにおける通信相手の相互認証方法及びその装置に関する。
【０００２】
【従来の技術】以下では、署名とは、デジタル署名を意味する。従来の相互認証方法にはＸ５０５６－３（ＩＳＯ／ＩＥＣ９７９８－３）５．２Ｍｕｔｕａｌ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ（相互認証）に定める相互認証プロトコルがあった。そのおもなプロトコルとしては、以下の２つがある。
・５．２．１　Two Pass Authentication
・５．２．２　Three Pass Authentication
また、相互認証プロトコルに対する主な攻撃（なりすまし）として、
・Man in the Middle 攻撃
・Replay攻撃
がある。
【０００３】まず、この従来の相互認証方法の概要を示す。
（１）５．２．１　Two Pass Authentication
図７ＡにTwo Pass Authentication の概要を示す。
１：通信装置ＳＴＡ１は相互認証プロトコルをおこなう時点の時刻をＴ１とし、［Ｔ１，ＳＴＡ２］に対する署名Ｓ１を生成する。
２：通信装置ＳＴＡ１は通信装置ＳＴＡ１の公開鍵ＰＫ１の証明書（ＰＫ１とＰＫ１に対する認証局の署名Ｂ１）とＴ１，ＳＴＡ２，Ｓ１とを通信装置ＳＴＡ２へ送る。（図７Ａの１）
３：通信装置ＳＴＡ２は通信装置１からＳＴＡ１の証明書Ｂ１を用いて署名Ｓ１を検査し、検査に不合格の場合はプロトコルを中断する。
４：通信装置ＳＴＡ２はプロトコルをおこなう時点の時刻をＴ２とし、［Ｔ２，ＳＴＡ１］に対する署名Ｓ２を生成する。
５：通信装置ＳＴＡ２は通信装置ＳＴＡ２の公開鍵ＰＫ２の証明書（ＰＫ１とその署名Ｂ２）、Ｔ２，ＳＴＡ１，Ｓ２を通信装置ＳＴＡ１へ送る。（図７Ａの２）
６：通信装置ＳＴＡ１は通信装置ＳＴＡ２からの証明書を用いて署名Ｓ２を検査し、検査に不合格の場合はプロトコルを中断する。
【０００４】３、６の検査が両方とも合格だった場合に、相互認証が成立する。
（２）５．２．２　Three Pass Authentication
図７ＢにThree Pass Authentication の概要を示す。
１：通信装置ＳＴＡ２は乱数Ｒ２を生成し、通信装置ＳＴＡ１へ送る。（図７Ｂの１）
２：通信装置ＳＴＡ１は乱数Ｒ１を生成し、［Ｒ１，Ｒ２，ＳＴＡ２］に対する署名Ｓ１を生成する。
３：通信装置ＳＴＡ１はその公開鍵ＰＫ１の証明書、Ｒ１，Ｒ２，ＳＴＡ２，Ｓ１を通信装置ＳＴＡ２へ送る。（図７Ｂの２）
４：通信装置ＳＴＡ２は通信装置ＳＴＡ１からの証明書を用いて署名Ｓ１を検査し、検査に不合格の場合はプロトコルを中断する。
５：通信装置ＳＴＡ２は［Ｒ２，Ｒ１，ＳＴＡ１］に対する署名Ｓ２を生成する。
６：通信装置ＳＴＡ２はその公開鍵ＰＫ２の証明書、Ｒ２，Ｒ１，ＳＴＡ１，Ｓ２を通信装置ＳＴＡ１へ送る。（図７Ｂの３）
７：通信装置ＳＴＡ１は通信装置ＳＴＡ２からの証明書を用いて署名Ｓ２を検査し、検査に不合格の場合はプロトコルを中断する。
【０００５】４、７の検査が両方とも合格だった場合に、相互認証が成立する。上記で説明した、従来の認証プロトコル

・５．２．１　Two Pass Authentication
・５．２．２　Three Pass Authentication
では、以下に説明するReplay攻撃を防ぐことはできるが、Man in the Middle 攻撃を防ぐことはできないという問題点がある。
・Man in the Middle 攻撃
通信装置ＳＴＡ１、ＳＴＡ２と平行して認証プロトコルを実行する能力を持つ不正通信者ＳＴＡ３が、通信装置ＳＴＡ１には不正通信者ＳＴＡ３通信装置（以下ＳＴＡ３は不正通信者又はその通信装置を意味する）が通信装置ＳＴＡ２であり、通信装置ＳＴＡ２には不正通信装置ＳＴＡ３が通信装置ＳＴＡ１であると信じさせることを目的とした攻撃方法である。
【０００６】認証プロトコル「５．２．１　Two Pass Authentication 」に対するMan in the Middle 攻撃は図８Ａのようになる。不正通信装置ＳＴＡ３は、通信装置ＳＴＡ１から送られてきたメッセージを通信装置ＳＴＡ２へ送り、通信装置ＳＴＡ２から送られてきたメッセージを通信装置ＳＴＡ１へ送ることによって、上記目的を果たすことができる。
１：通信装置ＳＴＡ１はプロトコルをおこなう時点の時刻をＴ１とし、［Ｔ１，ＳＴＡ２］に対する署名Ｓ１を生成する。
２：通信装置ＳＴＡ１はその公開鍵ＰＫ１の証明書、Ｔ１，ＳＴＡ２，Ｓ１を不正通信装置ＳＴＡ３へ送る。（図８Ａの１）
２ａ：不正通信装置ＳＴＡ３は通信装置ＳＴＡ１からの公開鍵ＰＫ１の証明書、Ｔ１，ＳＴＡ２，Ｓ１を通信装置ＳＴＡ２へ送る。（図８Ａの２）
３：通信装置ＳＴＡ２は通信装置ＳＴＡ１からの証明書を用いて署名Ｓ１を検査する。
４：通信装置ＳＴＡ２はプロトコルをおこなう時点の時刻をＴ２とし、［Ｔ２，ＳＴＡ１］に対する署名Ｓ２を生成する。
５：通信装置ＳＴＡ２はその公開鍵の証明書、Ｔ２，ＳＴＡ１，Ｓ２を不正通信装置ＳＴＡ３へ送る。（図８Ａの３）
５ａ：不正通信装置ＳＴＡ３は通信装置ＳＴＡ２からの公開鍵の証明書、Ｔ２，ＳＴＡ１，Ｓ２を通信装置ＳＴＡ１へ送る。（図８Ａの４）
６：通信装置ＳＴＡ１は通信装置ＳＴＡ２からの証明書を用いて署名Ｓ２を検査する。
【０００７】ここでは５．２．１　Two Pass Authentication について述べたが、５．２．２Three Pass Authentication に対しても同じ攻撃を行うことができる。
・Replay攻撃
不正通信者ＳＴＡ３が、通信装置ＳＴＡ２とＳＴＡ１の通信を傍受し、その情報を用いて、後の認証手順において通信装置ＳＴＡ２に不正通信装置ＳＴＡ３が通信装置ＳＴＡ１であると信じさせることを目的とした攻撃方法である。
【０００８】認証プロトコル「５．２．１　Two Pass Authentication 」に対するReplay攻撃は図８Ｂのようになる。まず、通信装置ＳＴＡ１とＳＴＡ２の認証プロトコルが行われ、これを不正通信装置ＳＴＡ３が盗聴する。
１：通信装置ＳＴＡ１はプロトコルをおこなう時点の時刻をＴ１とし、［Ｔ１，ＳＴＡ２］に対する署名Ｓ１を生成する。
２：通信装置ＳＴＡ１はその公開鍵ＰＫ１の証明書、Ｔ１，ＳＴＡ２，Ｓ１を通信装置ＳＴＡ２へ送る。（図８Ｂの１）
３：通信装置ＳＴＡ２は通信装置ＳＴＡ１からの証明書を用いて署名Ｓ１を検査し、検査に不合格の場合はプロトコルを中断する。
４：通信装置ＳＴＡ２はプロトコルをおこなう時点の時刻をＴ２とし、［Ｔ２，ＳＴＡ１］に対する署名Ｓ２を生成する。
５：通信装置ＳＴＡ２はその公開鍵ＰＫ２の証明書、Ｔ２，ＳＴＡ１，Ｓ２を通信装置ＳＴＡ１へ送る。（図８Ｂの２）
６：通信装置ＳＴＡ１は通信装置ＳＴＡ２からの証明書を用いて署名Ｓ２を検査し、検査に不合格の場合はプロトコルを中断する。
【０００９】つぎに通信装置ＳＴＡ１と（通信装置ＳＴＡ２であると偽った）不正通信装置ＳＴＡ３の認証プロトコルが行われる。
１：通信装置ＳＴＡ１はプロトコルをおこなう時点の時刻をＴ１´とし、［Ｔ１´，ＳＴＡ２］に対する署名Ｓ１を生成する。
２：通信装置ＳＴＡ１はその公開鍵ＰＫ１の証明書、Ｔ１´，ＳＴＡ２，Ｓ１を不正通信装置ＳＴＡ３へ送る。（図８Ｂの３）
３：不正通信装置ＳＴＡ３は通信装置ＳＴＡ１からの証明書を用いて署名Ｓ１を検査し、検査に不合格の場合はプロトコルを中断する。
４：不正通信装置ＳＴＡ３は先の盗聴により得た通信装置ＳＴＡ２の公開鍵ＰＫ２の証明書、Ｔ２，ＳＴＡ１，Ｓ２を通信装置ＳＴＡ１へ送る。（図８Ｂの４）
５：通信装置ＳＴＡ１は通信装置ＳＴＡ２の証明書を用いて署名Ｓ２を検査し、検査に不合格の場合はプロトコルを中断する。
【００１０】不正通信装置ＳＴＡ３は、通信装置ＳＴＡ２が送ったのと同じメッセージを通信装置ＳＴＡ１へ送るため、不正通信装置ＳＴＡ３は前回の認証時と同じ時刻情報Ｔ２を使うことになり、通信装置ＳＴＡ１は不正通信装置ＳＴＡ３が通信装置ＳＴＡ２でないことを見破ることができる。鍵共有したあと、暗号化したメッセージを交換して認証を行うことにより、Replay攻撃を防ぐことは可能である。

【００１１】しかし、不正通信者は、鍵共有プロトコルに対しても Man in the Middle攻撃を行うことにより、暗号化したメッセージを交換して認証を行う場合でも、なりすましをすることができる。また、
５．２．１　Two Pass Authentication
では、Replay攻撃に対する安全性を日時情報に依っているため、時刻情報を共有できない場合には完全ではなく、
５．２．２　Three Pass Authentication
では、メッセージのやりとりが１回増えて３回となるという問題がある。
【００１２】
【発明が解決しようとする課題】この発明の目的は、証明書を交換する認証方法の、Man in the middle と呼ばれる攻撃方法に対する弱点を解決し、しかも認証用のメッセージの交換の回数を減らして効率化した、認証方法及びその装置を提供することにある。
【００１３】
【課題を解決するための手段】この発明は、認証プロトコルの際に、証明書の交換に先だって交換される、鍵共有のための通信相手の装置が発生した乱数から算出された情報に対してデジタル署名を行うことを最も主要な特徴とする。従来技術とは、通信する両者が鍵共有を行う際に交換した情報を、認証プロトコルに用いる点が異なる。
【００１４】
【発明の実施の形態】実施形態１（請求項１）
図１Ａに、この実施形態１を実施した場合の認証方法（プロトコル）のシーケンスを示す。
①　最初の１往復の信号の送受で通信装置ＳＴＡ１、ＳＴＡ２が各々発生した乱数Ａ１，Ａ２から算出された値G^{A1}Mod Ｐ、G^{A2}Mod Ｐをそれぞれ認証要求、認証要求付に付けて相手局に送ることにより交換し、Diffie-Hellman鍵配送アルゴリズムにより秘密鍵ＫをＫ＝$G^{A1\cdot A2}$Mod Ｐと算出して共有する。
【００１５】なおＧ，ＰはDiffie-Hellman鍵配送アルゴリズムにおける公開鍵である。
②　共有して以降の信号の送受は、共有された秘密鍵Ｋを用いて暗号化されて行われる。したがって、鍵共有した当事者（ＳＴＡ１，ＳＴＡ２のいずれか）以外の第三者からの証明書の送信は、復号化処理により意味のないデータとなり、証明書の検証時に、排除することができる。以上により、証明書の送信者が、鍵共有を行った当事者であることが保証される。
③　通信装置ＳＴＡ１は署名用鍵Ｋ１に対する公開鍵ＰＫ１の証明書と、Diffie-Hellman鍵配送アルゴリズムで用いた情報G^{A2}Mod Ｐに対する署名用秘密鍵Ｋ１による署名を通信装置ＳＴＡ２へ送る。同様に通信装置ＳＴＡ２は署名用鍵Ｋ２に対する公開鍵ＰＫ２の証明書と、G^{A1}Mod Ｐに対する署名用秘密鍵Ｋ２による署名を通信装置ＳＴＡ１へ送る。
【００１６】このようにしてセッション時に生成されて送受された情報：ここでは、鍵共有用の情報G^{A1}Mod Ｐ、G^{A2}Mod Ｐに対して、証明書中の公開鍵に対応する署名用鍵によってデジタル署名できる能力を示すことにより、自分が、証明書を傍受して、不正に流用している通信者ではなく、証明書に記載されている公開鍵の本物の所有者であることを示す。
【００１７】つまり通信装置ＳＴＡ１は乱数を生成し、G^{A3}Mod Ｐを演算し、認証要求とG^{A3}Mod Ｐを不正通信装置ＳＴＡ３へ送り、不正通信装置ＳＴＡ３は乱数Ａ４を生成し、G^{A4}Mod Ｐを演算し、これと認証要求受付とを通信装置ＳＴＡ１へ送る。両通信装置ＳＴＡ１、ＳＴＡ３はそれぞれ秘密鍵Ｋ′＝$G^{A3\cdot A4}$Mod Ｐを計算する。
【００１８】次に共通した秘密鍵Ｋ′で暗号化して送受信を行うが不正通信装置ＳＴＡ３は傍受した通信装置ＳＴＡ２の公開鍵ＰＫ２の証明書を用いてこれを通信装置ＳＴＡ１に送ることができるが、通信装置ＳＴＡ２のＰＫ２と対応する署名用鍵Ｋ２を知らないため、G^{A1}Mod Ｐに対する正しい署名を通信装置ＳＴＡ１へ送ることができない。
【００１９】従って通信装置ＳＴＡ１は、公開鍵ＰＫ２が正しいものであることを確認することができるが、このＰＫ２を用いて、不正通信装置ＳＴＡ３よりのG^{A1}Mod Ｐに対する署名と相当するものを検証した際に、不合格となり、秘密鍵Ｋ′を共有した相手が通信装置ＳＴＡ２でないことが判明する。
④　検証結果及び接続条件によって接続の可否を判断する。
【００２０】上記により、鍵を共有した相手が証明書の送信者であり、かつ、証明書に記載されている公開鍵と対応する署名用鍵Ｋ１，Ｋ２を知っていることが相互に証明できる。この実施の形態において、Diffie-Hellman鍵配送アルゴリズムの代わりに、楕円Diffie-Hellman鍵配送アルゴリズムを使用することが可能である。
【００２１】実施形態２（請求項２）
公開鍵暗号（ＲＳＡ暗号、Ｅｌ Ｇａｍａｌ暗号、など）を用いて鍵Ａ２を共有し、鍵Ａ２を用いた暗号通信を行っている状態でデジタル署名を用いた認証プロトコルを行う場合を想定している。ここで、鍵共有に用いる公開鍵暗号の公開鍵にたいしても認証局が証明書を発行することにより、鍵共有と認証を同時に行う方法も考えられるが、
・鍵共有用と署名用に別々の証明書を必要とする方式は、認証局の負担が増えること。
・認証プロトコルは暗号化した状態で行った方が不特定多数に認証用の情報が漏れる危険が減ること。
などの理由から、「鍵共有プロトコル」「暗号通信で認証プロトコル」という順に行うのが一般的である。

【００２２】図２にこの実施形態の認証プロトコルのシーケンスを示す。
公開鍵暗号用の公開鍵ＰＫとデジタル署名用の公開鍵ＰＫ１またはＰＫ２は同じでも異なっていても良いが、
・署名と暗号に同じ鍵を用いると、安全性に問題が有る場合がある。
・署名／暗号両用のアルゴリズムに比較して、どちらか片方しか出来ないアルゴリズムにより高速なものが存在する
という理由から、一般には異なる公開鍵を用いる。
① 最初の１往復の信号の送受で通信装置ＳＴＡ１は、通信装置ＳＴＡ２に通信装置ＳＴＡ１の公開鍵ＰＫを認証要求と共に送信し、通信装置ＳＴＡ２は、乱数Ａ２を発生し、公開鍵ＰＫによって乱数Ａ２を暗号化した値Ｓ２と認証要求受付を通信装置ＳＴＡ１に送り返す。
【００２３】通信装置ＳＴＡ１はＳ２を復号して乱数Ａ２を得る。以後、メッセージを暗号化する鍵としてＡ２を用いる。
② 共有して以降の信号の送受は、共有された鍵Ａ２を用いて暗号化されて行われる。Ａ2は、（ａ）発生した通信装置ＳＴＡ２と、（ｂ）公開鍵ＰＫに対応する秘密鍵ＳＫを持っており、公開鍵ＰＫによる暗号文を復号できる通信装置のみが知りえる情報である。
【００２４】したがって、鍵共有した当事者（ＳＴＡ１，ＳＴＡ２のいずれか）以外の第三者からの証明書の送信は、復号化処理により意味のないデータとなり、証明書の検証時に、排除することができる。以上により、証明書の送信者が、鍵共有を行った当事者であることが保証される。
③ 通信装置ＳＴＡ１は、乱数Ａ１を発生し、
・通信装置ＳＴＡ１の公開鍵ＰＫ１の証明書、
・通信装置ＳＴＡ１の秘密鍵Ｋ１による、［Ａ１，Ｓ２］に対する署名
・Ａ１，Ｓ２
を通信装置ＳＴＡ２に送る。
【００２５】通信装置ＳＴＡ２は、
・通信装置ＳＴＡ２の公開鍵ＰＫ２の証明書
・通信装置ＳＴＡ２の秘密鍵Ｋ２による［Ｓ２，Ａ１］に対する署名
・Ｓ２，Ａ１
を通信装置ＳＴＡ１に送る。
【００２６】ここで、ＳＴＡ１→ＳＴＡ２のときと、ＳＴＡ２→ＳＴＡ１の時で、Ｓ２とＡ１の順番が逆になっているのは、従来法であるＸ５０５６－３（ＩＳＯ／ＩＥＣ９７９８－３）５．２．２Three Pass Authentication の該当する部分にならっている。両方とも同じ順番にしても良い。このような処理により、実施の形態１と同様、セッション時に生成されて送受された予測不可能な情報：ここでは、Ａ１，Ｓ２を、証明書中の公開鍵に対応する署名用鍵によってデジタル署名できる能力を示すことにより、自分が、証明書を傍受して、不正に流用している通信者ではなく、証明書に記載されている公開鍵の本物の所有者であることを示している。
④ 検証結果及び接続条件によって接続の可否を判断する。
【００２７】上記により、鍵を共有した相手が証明書の送信者であり、かつ、証明書に記載されている公開鍵と対応する秘密鍵Ｋ１，Ｋ２を知っていることが相互に証明できる。この実施形態は、公開鍵暗号一般（ＲＳＡ、ＥｌＧａｍａｌ、楕円ＥｌＧａｍａｌ、ラビン）による鍵配送方式に適用可能である。
【００２８】実施形態１に用いられる通信装置ＳＴＡ１の機能構成例を図３に示す。記憶部１１には乱数生成部ノイズ生成された乱数Ａ１、鍵配送アルゴリズムに用いられる公開情報Ｇ，Ｐ、共有鍵生成部１３で生成された共有鍵ＳＫ、その通信装置ＳＴＡ１の公開鍵ＰＫ１の証明書、そのＰＫ１と対の署名用秘密鍵Ｋ１、相手通信装置ＳＴＡ２から送られた鍵配送用関数値結果Ｇ（Ａ２）などが記憶されている。
【００２９】関数演算部１４では乱数Ａ１、公開情報Ｐ，Ｇが入力されて鍵配送アルゴリズムによる鍵配送用関数Ｆ（Ａ１）が演算される。つまり、鍵配送アルゴリズムは必ずしもDiffie-Hellmanのアルゴリズムに限らず、要は乱数Ａ１を変数とした関数を利用するものであればよい。共有鍵生成部１３では相手通信装置ＳＴＡ２からの鍵配送用関数値Ｇ（Ａ２）と、乱数Ａ１とから共有の秘密鍵ＳＫを生成して、記憶部１１に記憶する。
【００３０】前記実施例ではＧ（Ａ２）に対し、Ｋ１による署名を直接行ったが、Ｇ（Ａ２）を変数とする関数Ｈ（Ｇ（Ａ２））、例えばＧ（Ａ２）を整数倍した簡単な関数や、複数次数の複雑な関数でもよい。更に乱数Ａ１も付加したものでもよい。単純にはＡ１＋Ｇ（Ａ２）自体又はＨ（Ａ１＋Ｇ（Ａ２））としてもよい。よってこの例では認証用演算部１５でＧ（Ａ２）とＡ１を変数として関数Ｈ（Ａ１，Ｇ（Ａ２））を演算し、その演算結果に対し、署名部１６で、署名用秘密鍵Ｋ１によりデジタル署名がなされる。
【００３１】その暗号部１７では署名部１６の署名結果、つまり認証用署名Ｃ１と、公開鍵ＰＫ１の証明書に対し、または検証結果生成部１８からの検証結果に対し、共有鍵ＳＫで暗号化する。認証要求と鍵配送用関数演算部１４用演算結果Ｆ（Ａ１）、や暗号部１７の暗号化出力が送信部１９により通信装置ＳＴＡ２など相手通信装置へ送信される。
【００３２】通信装置ＳＴＡ２からなど外部からの信号が受信部２０で受信され、それが認証要求受付けの場合は、Ｇ（Ａ２）が共有鍵生成部１３へ入力され、共有鍵ＳＫを生成以後の受信信号は復号部２１で共有鍵ＳＫで復号される。復号部２１の出力中の公開鍵ＰＫ２の証明書に対し、公開鍵確認部２２でその受信公開鍵ＰＫ２が

正しいものであることが確認され、その確認された公開鍵ＰＫ２を用いて、受信された認証用署名Ｃ２が署名検証部２３で検証される。公開鍵確認部２２、署名検証部２３の各検証結果にもとづき、検証結果生成部１８で検証結果が生成される。以上の各部に対する制御、その処理実行が制御部２４により行われる。一般には、これらの処理はコンピュータにより行われる。

【００３３】図４に図２に示した実施形態２の通信装置ＳＴＡ１の機能構成を図３と対応する部分に同一符号を付けて示す。この場合記憶部１１には鍵配送用公開鍵α（図２ではＰＫ）、が鍵配送用公開情報Ｐ，Ｇの代りに記憶され、またＧ（Ａ２）の代りに暗号情報Ｇ（α、Ａ２）＝Ｓ２が記憶される。鍵配送処理時には、記憶要求と鍵配送用公開鍵αとが送信され、また受信部２０で受信された鍵配送時の暗号情報Ｇ（α、Ａ２）は共有鍵生成部１３で公開鍵αで復号され、前記実施例ではＡ２が共有鍵ＳＫとされて記憶部１１に記憶される。しかし、この共有鍵ＳＫはＡ２の関数であればよい。また認証処理において、乱数生成部２６から乱数Ａ１を生成し、（Ｓ２＝Ｇ（α、Ａ２），Ａ２）に対し直接署名用秘密鍵Ｋ１で署名したが、図３の場合と同様に認証用関数演算部１５でＨ（Ａ１，Ｓ２）を演算し、これに対し、署名部１６でＫ１による署名を行ってもよい。その他は図３の場合と同一である。

【００３４】この実施形態２における通信装置ＳＴＡ２の場合は図４に破線で示すように、鍵配送時に、乱数生成部２７で乱数Ａ２が生成され、その乱数Ａ２に対し暗号部２８で公開鍵αにより暗号化されＧ（α、Ａ２）とされて送信される。共有鍵生成部ではＡ２とαから共有鍵ＳＫが生成される。その他は通信装置ＳＴＡ１と同様である。通信装置ＳＴＡ１，ＳＴＡ２は何れが先に認証要求を出すかは不明であるから通信装置としては両機能を具備する。

【００３５】図１乃至図４において共有鍵ＳＫの生成後は、その共有鍵ＳＫにより全ての送信情報と暗号化して送信し、受信情報をＳＫで復号すると述べたが、前記相互認証処理、つまり図１、図２に対する説明中の❸，❹においては共有鍵ＳＫにより暗号化を行うことなく相互認証を行ってもよい。

【００３６】

【発明の効果】この発明を実施すると、証明書の送信者が、証明書に記載されている公開鍵と対応する秘密鍵を知っていることの証明が行えるのと同時に、不正な第三者によるMan in the middle 攻撃の防止を、２－ｐａｔｈのメッセージ交換によって行うことができる。

【００３７】この発明の実施形態１（図１）において、不正な第三者ＳＴＡ３がMan in themiddle 攻撃を試みている状況を図５に示す。不正通信装置ＳＴＡ３は通信装置ＳＴＡ２に対しては通信装置ＳＴＡ１になりすまし、通信装置ＳＴＡ１に対しては通信装置ＳＴＡ２になりすますために、通信装置ＳＴＡ１からのメッセージを中継して通信装置ＳＴＡ２に送り、通信装置ＳＴＡ２からのメッセージを中継して通信装置ＳＴＡ１に送る。

【００３８】この発明手順において、なりすましを実行するために、不正通信装置ＳＴＡ３は以下の❶、❷、❸、❹を行うことが必要である。鍵の共有のためのシーケンスの１番目と２番目のメッセージにおいては：

❶通信装置ＳＴＡ１にはＦ（Ａ２）の代わりに自分で発生した乱数Ａ３から関数Ｈによって算出されるＨ（Ａ３）を送る。

❷通信装置ＳＴＡ２にはＦ（Ａ２）の代わりに自分で発生した乱数Ａ４から数Ｉによって算出されるＩ（Ａ４）を送る。

【００３９】なお❶と❷を行わないで、Ｆ（Ａ１）を通信装置ＳＴＡ２に、Ｇ（Ａ２）を通信装置ＳＴＡ１に単に中継すると、通信装置ＳＴＡ１とＳＴＡ２は不正通信装置ＳＴＡ３には知りえない秘密鍵ＳＫを共有出来ることになり、不正通信装置ＳＴＡ３が通信装置ＳＴＡ１、ＳＴＡ２なりすますことができない。認証の１－ｐａｔｈ目のシーケンスの３番目と４番目のメッセージにおいては：

❸不正通信装置ＳＴＡ３は通信装置ＳＴＡ２が送信したＧ（Ａ２）に対して、通信装置ＳＴＡ１のデジタル署名用鍵Ｋ１を用いてデジタル署名（Ｓｉｇ１）して通信装置ＳＴＡ２に、Ｋ１に対応する公開鍵ＰＫ１の証明書とともに送る。

❹不正通信装置ＳＴＡ３は通信装置ＳＴＡ１が発生したＦ（Ａ１）に対して、通信装置ＳＴＡ２のデジタル署名用鍵Ｋ２を用いてデジタル署名（Ｓｉｇ２）して通信装置ＳＴＡ１にＫ２に対応する公開鍵ＰＫ２の証明書とともに送る。

【００４０】しかしながら、

（１）不正通信装置ＳＴＡ３は証明書に記載されたデジタル署名用鍵Ｋ１，Ｋ２を知らない

（２）通信装置ＳＴＡ１のところには、Ｆ（Ａ２）は届かない

（３）通信装置ＳＴＡ２のところにはＦ（Ａ１）は届かない

ため、不正通信装置ＳＴＡ３にはＳｉｇ１、Ｓｉｇ２を正しく偽造して送信することは不可能である。

【００４１】次に、この発明の実施形態２（図２）において、不正な第三者ＳＴＡ３がManin the middle 攻撃を試みている状況を図６に示す。この状況において、不正通信装置ＳＴＡ３が、通信装置ＳＴＡ１，ＳＴＡ２になりすますためには、鍵配送のために送受した、乱数Ａ２，Ａ３の通信装置ＳＴＡ１、ＳＴＡ３の公開鍵による署名Ｓ３、Ｓ２を、通信装置ＳＴＡ１，ＳＴＡ２の秘密鍵Ｋ１，Ｋ２を用いて署名できることが必要であるが、不正通信装置ＳＴＡ３はＫ１，Ｋ２を知らないので、これは不可能である。

【００４２】上記により、この発明がMan in the middle 攻撃に対して有効であることが示せた。また、この発明は共有鍵による暗号通信が前提であって、その共有鍵の配送処理において利用した情報を相互認証に用いるため、メッセージの送信回数は２回で済み、効率的に認証を行うことができる。

【図面の簡単な説明】

【図１】この発明の実施例の認証プロトコルのシーケンスと不正な第三者ＳＴＡ３がReplay攻撃を試みている状況を示す図。

【図２】この発明を実施例２の認証プロトコルのシーケンスを示す図。

【図３】実施例１の通信装置の機能構成例を示すブロック図。

【図４】実施例２の通信装置の機能構成例を示すブロック図。

【図５】請求項１において、不正な第三者ＳＴＡ３がMan in the middle 攻撃を試みている状況を示す図。

【図６】本発明請求項４において、不正な第三者ＳＴＡ３がMan in the middle 攻撃を試みている状況を示す図。

【図７】ＡはTwo Pass Authentication の概要を示す図、ＢはThree Pass Authentication の概要を示す図である。

【図８】ＡはMan in the middle 攻撃を概要を示す図、ＢはReplay攻撃の概要を示す図である。

【図２】

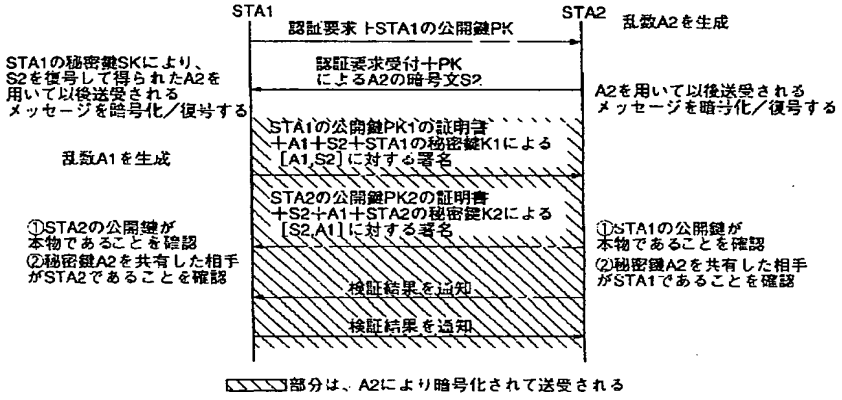


図 2

【図４】

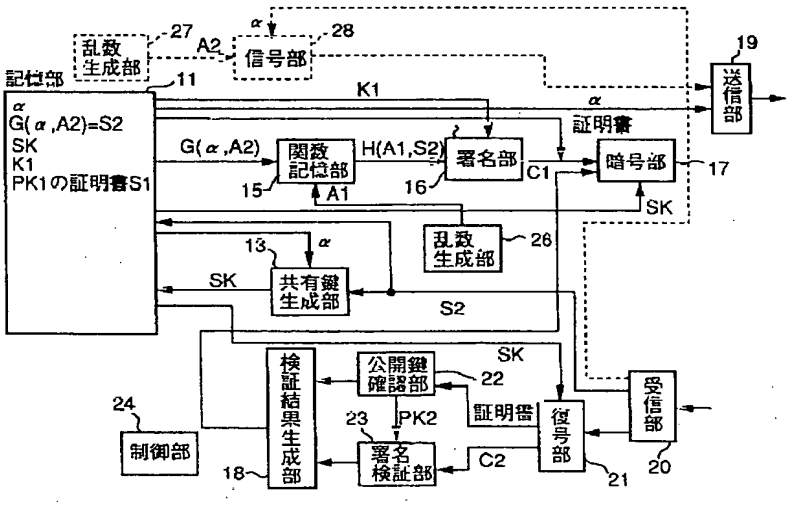


図 4

【図1】

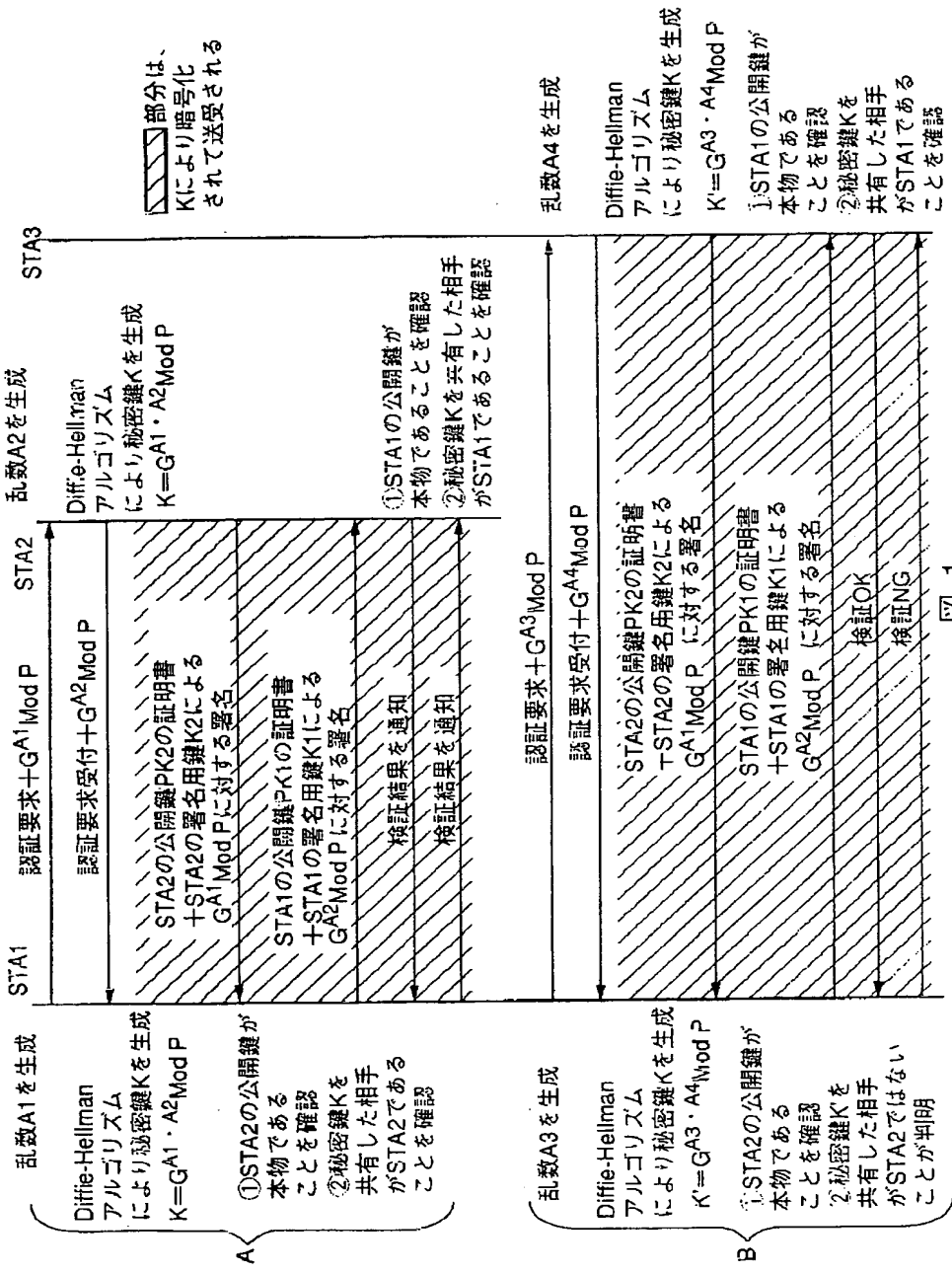

STA1
STA2
STA3
乱数A1を生成
認証要求＋G^{A1}Mod P
乱数A2を生成
Diffie-Hellman
アルゴリズム
により秘密鍵Kを生成
$K=G^{A1}\cdot A2$Mod P
認証要求受付＋G^{A2}Mod P
STA2の公開鍵PK2の証明書
＋STA2の署名用鍵K2による
G^{A1}Mod Pに対する署名
STA1の公開鍵PK1の証明書
＋STA1の署名用鍵K1による
G^{A2}Mod Pに対する署名
検証結果を通知
検証結果を通知
①STA2の公開鍵が
本物であること
を確認
②秘密鍵Kを
共有した相手
がSTA2であること
を確認
A
乱数A3を生成
Diffie-Hellman
アルゴリズム
により秘密鍵K'を生成
$K'=G^{A3}\cdot A4$Mod P
①STA2の公開鍵が
本物であること
を確認
②秘密鍵K'を
共有した相手
がSTA2ではないこと
が判明
B
乱数A4を生成
Diffie-Hellman
アルゴリズム
により秘密鍵Kを生成
$K'=G^{A3}\cdot A4$Mod P
①STA1の公開鍵が
本物であること
を確認
②秘密鍵Kを
共有した相手
がSTA1であること
を確認
認証要求＋G^{A3}Mod P
認証要求受付＋G^{A4}Mod P
STA2の公開鍵PK2の証明書
＋STA2の署名用鍵K2による
G^{A1}Mod Pに対する署名
STA1の公開鍵PK1の証明書
＋STA1の署名用鍵K1による
G^{A2}Mod Pに対する署名
検証OK
検証NG
部分は、
Kにより暗号化
されて送受される

図 1

【図3】

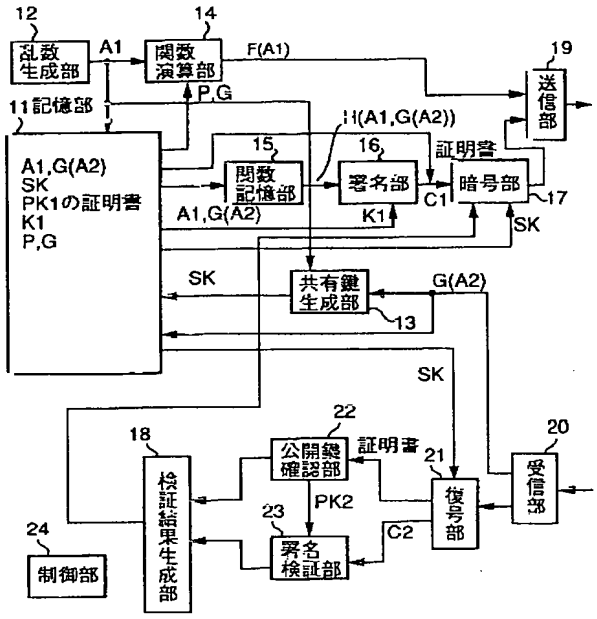

12
乱数生成部
A1
14
関数演算部
F(A1)
19
送信部
P,G
11記憶部
H(A1,G(A2))
15
関数記憶部
16
署名部
証明書
暗号部
17
A1,G(A2)
SK
PK1の証明書
K1
P,G
A1,G(A2)
K1
C1
SK
SK
共有鍵生成部
G(A2)
13
SK
22
公開鍵確認部
証明書
21
20
受信部
18
検証結果生成部
PK2
復号部
23
署名検証部
C2
24
制御部

図 3

【図5】

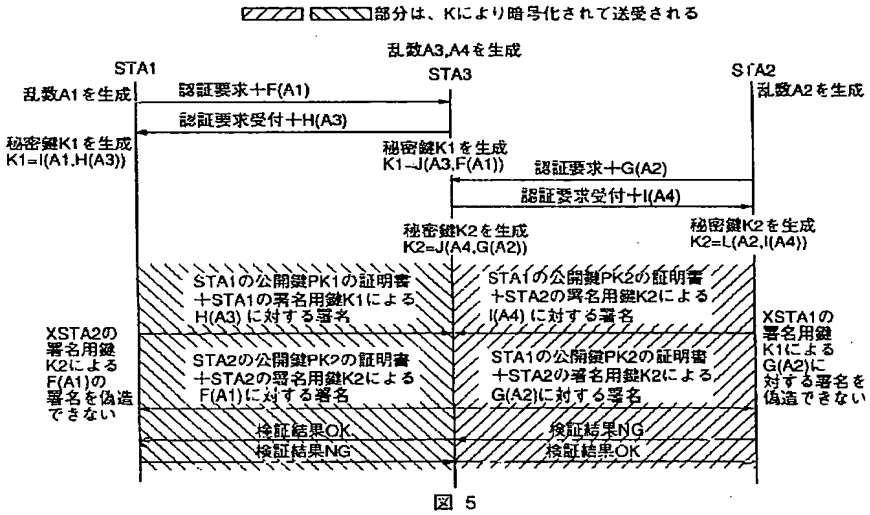

部分は、Kにより暗号化されて送受される
乱数A3,A4を生成
STA1
STA3
STA2
乱数A1を生成
認証要求+F(A1)
認証要求受付+H(A3)
乱数A2を生成
秘密鍵K1を生成
K1=I(A1,H(A3))
秘密鍵K1を生成
K1=J(A3,F(A1))
認証要求+G(A2)
認証要求受付+I(A4)
秘密鍵K2を生成
K2=J(A4,G(A2))
秘密鍵K2を生成
K2=L(A2,I(A4))
STA1の公開鍵PK1の証明書
+STA1の署名用鍵K1による
H(A3)に対する署名
STA1の公開鍵PK2の証明書
+STA2の署名用鍵K2による
I(A4)に対する署名
XSTA2の署名用鍵K2によるF(A1)の署名を偽造できない
STA2の公開鍵PK2の証明書
+STA2の署名用鍵K2による
F(A1)に対する署名
STA1の公開鍵PK2の証明書
+STA2の署名用鍵K2による
G(A2)に対する署名
XSTA1の署名用鍵K1によるG(A2)に対する署名を偽造できない
検証結果OK
検証結果NG
検証結果NG
検証結果OK

図 5

【図6】

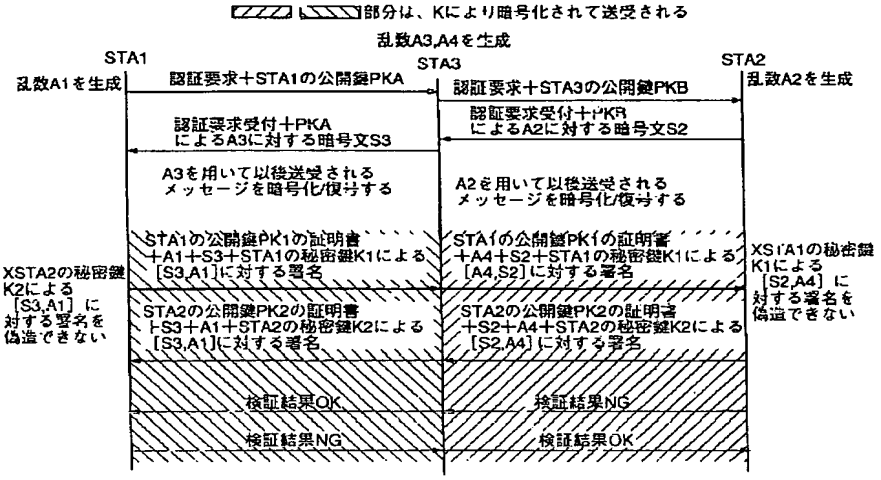


図 6

【図7】

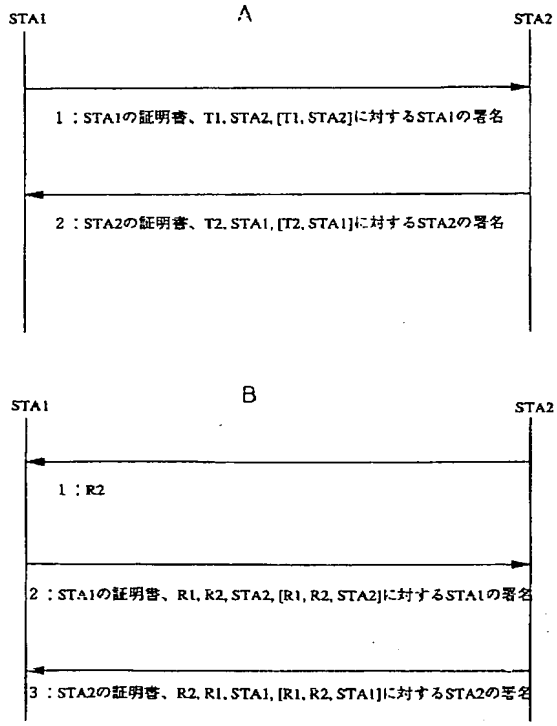


図 7

【図8】

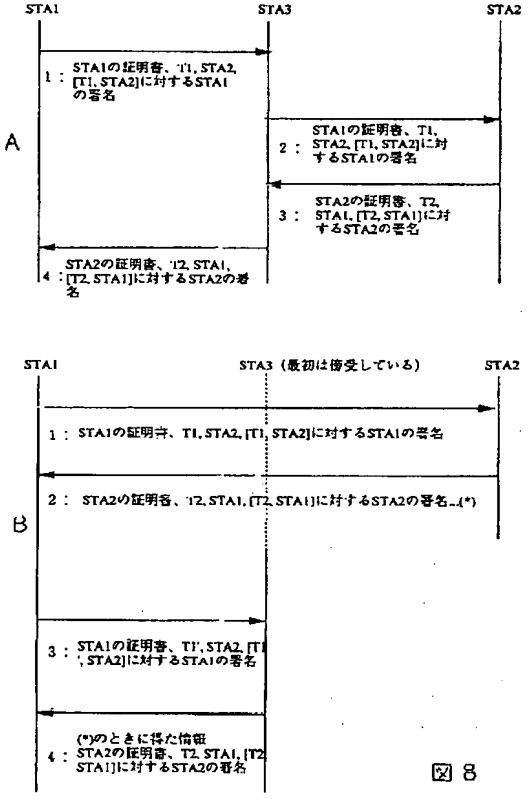


図 8